UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/402,144	09/29/1999	MARTINA HANCK	P991784	5593

29177 7590 05/09/2008

BELL, BOYD & LLOYD, LLP
P.O. BOX 1135
CHICAGO, IL 60690

EXAMINER	
KIM, JUNG W	

ART UNIT	PAPER NUMBER
2132	

MAIL DATE	DELIVERY MODE
05/09/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/402,144
Filing Date: September 29, 1999
Appellant(s): HANCK ET AL.

Jeffrey J. Howell
Reg. No. 46,402
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 1/28/08 appealing from the Office action mailed 6/27/07.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

5,649,089	KILNER	7-1997
4,982,430	FREZZA ET AL.	1-1991

4,533,948 MCNAMARA ET AL. 8-1985

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 103

Claims 1-3, 10-12, 22-33 and 37-48 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kilner USPN 5,649,089 in view of Frezza et al. U.S. Patent No. 4,982,430 (hereinafter Frezza); subject matter in McNamara et al. USPN 4,533,948 is relied upon since the McNamara patent is incorporated by reference into the Frezza patent (hereinafter McNamara).

As per claim 10, Kilner discloses an arrangement for forming a first commutative checksum for digital data which are grouped into a number of data segments, the arrangement comprising:

an arithmetic and logic unit, (fig. 1, reference nos. 112 and 115)

a first segment checksum, which is formed for each of the data segment in accordance with a type selected from the group consisting of a hashing value and a cryptographic one-way function, (fig. 1, reference no. 124)

a commutative operation which forms the first commutative checksum by operating on the segment checksums, wherein flow control for the data segments is negated by the commutative operation (fig. 1, reference no. 130; irrespective of

the order the data is received and stored into the database, A_CRC, V_CRC and S_CRC values remains the same)

Kilner does not disclose a cryptographic operation to protect the first commutative checksum. Frezza teaches encrypting integrity values prior to submitting the integrity value over a network link to prevent unauthorized alteration of a message. Frezza, col. 2:45-3:13. It would be obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Kilner by including a cryptographic operation to secure the first commutative checksum. One would be motivated to do so to prevent an unscrupulous third party from an unauthorized modification of a transmitted message (Frezza, col. 2:20-25). The aforementioned cover the limitations of claim 10.

As per claim 12, the rejection of claim 10 under 35 USC 103(a) as being unpatentable over Kilner in view of Frezza is incorporated herein. In addition, the arrangement also includes the following:

an inverse cryptographic operation to form a first commutative checksum from the cryptographic commutative checksum, (Frezza, col. 1:12-19; 5:50-58; McNamara, 7:34-42; 8:25-35; data encrypted by DES has an inverse operation to retrieve the original data; furthermore, every ciphertext is associated with a specific plaintext);

a second segment checksum which is formed for each of the data segment of the digital data to which the first commutative checksum is allocated,

a commutative operation which operates on the second segment checksum which forms a second commutative checksum wherein flow control for the data segments is negated by the commutative operation, and a comparator which checks for a match between the second commutative checksum and a reconstructed first commutative checksum, wherein the first and second segment checksum are formed in accordance with a type selected from the group consisting of a hashing value and a cryptographic one-way function. (Kilner, 5:5:48-6:15; fig. 3, reference nos. 311 and 312; resync operation regenerates S_CRC; S_CRC is compared with V_CRC. Because the first commutative checksum uses first segment checksums for each data segment using a CRC technique, the second commutative checksum, which is used to verify the validity of the first commutative checksum, also generates second segment checksums for each data segment using a CRC technique).

It would be obvious to one of ordinary skill in the art at the time the invention was made to implement a cryptographic operation to secure the first commutative checksum. One would be motivated to do so to prevent an unscrupulous third party from an unauthorized modification of a transmitted message (Frezza, col. 2:20-25). The aforementioned cover the limitations of claim 12.

As per claim 11, it is a claim corresponding to claim 12, and it does not teach or define above the information claimed in claim 12. Therefore, claim 11 is rejected as

being unpatentable over Kilner in view of Frezza for the same reasons set forth in the rejection of claim 12.

As per claim 37, Kilner in view of Frezza cover the following: 1) an arrangement for forming a first commutative checksum, 2) an arrangement for checking a predetermined cryptographic commutative checksum, and 3) an arrangement for forming and checking a first commutative checksum as outlined above in the claim 10 rejection 35 U.S.C. 103(a). In addition, the cryptographic operations described use a symmetric key methodology (Frezza, col. 1:12-19; 5:50-58; McNamara, 7:34-42; 8:25-35).

As per claims 38 and 39, Kilner in view of Frezza cover the following: 1) an arrangement for forming a first commutative checksum, 2) an arrangement for checking a predetermined cryptographic commutative checksum, and 3) an arrangement for forming and checking a first commutative checksum as outlined above in the claim 11 and 12 rejections under 35 U.S.C. 103(a). In addition, the cryptographic operations described use a symmetric key methodology (Frezza, col. 1:12-19; 5:50-58; McNamara, 7:34-42; 8:25-35). The aforementioned cover the limitations of claims 38 and 39.

As per claims 40, Kilner in view of Frezza cover the following: 1) an arrangement for forming a first commutative checksum, 2) an arrangement for checking a predetermined cryptographic commutative checksum, and 3) an arrangement for

forming and checking a first commutative checksum as outlined above in the claim 10 rejection under 35 U.S.C. 103(a). In addition, Kilner teaches the commutative operation to establish column parity, which forms the commutative checksums, is an XOR operation (Kilner, col. 3:52-65): the XOR operation exhibits both commutative and associative properties. The aforementioned cover the limitation of claim 40.

As per claims 41 and 42, Kilner in view of Frezza cover the following: 1) an arrangement for forming a first commutative checksum, 2) an arrangement for checking a predetermined cryptographic commutative checksum, and 3) an arrangement for forming and checking a first commutative checksum as outlined above in the claim 11 and 12 rejections under 35 U.S.C. 103(a). In addition, Kilner teaches the commutative operation to establish column parity, which forms the commutative checksums, is an XOR operation (Kilner, col. 3:52-65): the XOR operation exhibits both commutative and associative properties. The aforementioned cover the limitations of claims 41 and 42.

As per claim 43, Kilner in view of Frezza cover an arrangement as outlined above in the claim 10 rejection under 35 U.S.C. 103(a). Kilner does not expressly disclose archiving the digital data and the cryptographic commutative checksum. However, archiving the elements of a transmission is a standard feature to verify the contents of a transmission to an auditor. The examiner takes Official Notice that archiving transmission elements are standard means to record the transmission to prove the contents and status of the transmission at a latter date (i.e. auditing a transmission). It

would be obvious to one of ordinary skill in the art at the time the invention was made to archive the digital data and the checksum since it preserves a receipt of the transmission. The aforementioned cover the limitations of claim 43.

As per claims 44 and 45, Kilner in view of Frezza cover an arrangement as outlined above in the claim 11 and 12 rejections under 35 U.S.C. 103(a). Kilner does not expressly disclose archiving the digital data and the cryptographic commutative checksum. However, archiving the elements of a transmission is a standard feature to verify the contents of a transmission to an auditor. The examiner takes Official Notice that archiving transmission elements are standard means to record the transmission to prove the contents and status of the transmission at a latter date (i.e. auditing a transmission). It would be obvious to one of ordinary skill in the art at the time the invention was made to archive the digital data and the checksum since it preserves a receipt of the transmission. The aforementioned cover the limitations of claims 44 and 45.

As per claim 46, Kilner in view of Frezza cover the following: 1) an arrangement for forming a first commutative checksum, 2) an arrangement for checking a predetermined cryptographic commutative checksum, and 3) an arrangement for forming and checking a first commutative checksum as outlined above in the claim 10 rejections under 35 U.S.C. 103(a). In addition, as mentioned previously, the digital data is cryptographically protected, and by convention, the cryptographic operation would be

implemented by an ALU. Furthermore, since Kilner discloses sending the digital data as well as the checksum values and commutative checksum value from the active database to a standby database over a network link (col. 3:14-19, and figs.1-4), and Frezza teaches securing the integrity value being transmitting over a digital network, the digital data would necessarily be processed in accordance with a network management protocol. The aforementioned cover the limitation of claim 46.

As per claims 47 and 48, Kilner in view of Frezza cover the following: 1) an arrangement for forming a first commutative checksum, 2) an arrangement for checking a predetermined cryptographic commutative checksum, and 3) an arrangement for forming and checking a first commutative checksum as outlined above in the claim 11 and 12 rejections under 35 U.S.C. 103(a). In addition, as mentioned previously, the digital data is cryptographically protected, and by convention, the cryptographic operation would be implemented by an ALU. Furthermore, since Kilner discloses sending the digital data as well as the checksum values and commutative checksum value from the active database to a standby database over a network link (col. 3:14-19, and figs.1-4), and Frezza teaches securing the integrity value being transmitting over a digital network, the digital data would necessarily be processed in accordance with a network management protocol. The aforementioned cover the limitations of claims 47 and 48.

As per claims 1-3 and 22-33, they are method claims corresponding to the subject matter covered in the rejections of claims 10-12 and 37-48, and they do not teach or define above the information covered in the rejections of claims 10-12 and 37-48. Therefore, claims 1-3 and 22-33 are rejected under Kilner in view of Frezza for the same reasons set forth in the rejections of claims 10-12 and 37-48.

(10) Response to Argument

On pgs. 12-13 of Appellant's Appeal Brief, Appellant argues that the commutative checksum of the claimed invention is distinguished from the cumulative checksum of the Kilner prior art. In particular, Appellant argues:

> The Office Action cites col. 3, lines 52-55 and the XOR operation as the equivalent of the claimed commutative checksum. However, Appellant points out that the XOR operation is only applied to the reversible incorporation of record checksums (R_CRC), where the checksums are "backed in" and "backed out" of the A_CRC checksum, which is disclosed as the "cumulative checksum of the entire DB for substantially real time tracking changes to a database" (col. 3, lines 53-55). The R_CRC checksum then, must rely on flow control, since the individual records must be ordered to update the record numbers in the A_CRC (col. 4, lines 27-54)

As an initial matter, the limitation in the independent claims that the Appellant is distinguishing from the prior art is the "wherein" clause, which describes a characteristic of the commutative operation ("wherein flow control for the data segments is negated by the commutative operation"; see exemplary claim 1). In the Appeal Brief, Appellant has cited pg. 2, lines 14-26 of the specification as providing support for this limitation. See

Appeal Brief, pg. 6, last paragraph. This portion of the specification is replicated here in full:

> Commutative operations are known. Kiyek & Schwarz include a general definition for commutative operations, which can be understood to be an operation in which the order of individual operations is unimportant and any order of individual operations always leads to the same total operation. A commutative operation can be, for example, an exclusive or (EXOR), an additive operation or also a multiplicative operation. A method and a device for generating check code segments for the occurrence of source data and for determining errors in the source data are known.

Based on Appellant's citation, it appears that the claim limitation in question is describing the following characteristic of the commutative operations: the operations must enable the first commutative checksum to be validated without performing the operations in a certain order. Other portions of the specification also point to this characteristic (see also, pg. 4, lines 23-34).

In view of this interpretation of the claim limitation, Appellant's conclusion that the R_CRC disclosed by Kilner must rely on flow control is not correct. Kilner discloses steps to establish and maintain an A_CRC, which is the cumulative checksum for the active database, wherein each record of the active database has a corresponding record checksum (R_CRC). Col. 3, lines 52-65. Each R_CRC is incorporated reversibly into the A_CRC by shifting its CRC-16 left by its record number modulo 16 and XOR-ing it into the cumulative checksum. Id. When a record is changed, the old R_CRC corresponding to the record prior to the change is backed out by performing the same process, and the new R_CRC for the updated record is backed in. Col. 4, lines 40-45. After each update of a record in the active database, an update or

resynchronization message containing the old R_CRC and the new record value is streamed to the standby database *without acknowledgement*. Col. 4, lines 10-17. Accordingly, a V_CRC is updated by the active database, which is representative of what the CRC value the active database expects the standby database to have. Col. 4, lines 18-20. At the standby database, the corresponding records are updated upon receipt of each update message sent from the Active database. Col. 6, lines 5-8. After a new record is updated, the old R_CRC value is backed out from the standby cumulative checksum (S_CRC), and then the new R_CRC is backed into the S_CRC. Col. 6, lines 8-11. Because both the A_CRC and S_CRC are generated by XOR-ing the individual record checksums, these cumulative checksums are equivalent to the "commutative checksums" defined by Appellant's claims; i.e. the value of the cumulative checksums are not dependent on the order of integrating the individual record checksums, i.e. XOR is a commutative operation. In addition, there is no description in Kilner of a flow control mechanism. Once an update message is submitted by the active database, the standby database does not discern the relative ordering of the update messages received; the standby database updates the records on a first come first serve basis. Therefore, contrary to Appellant's allegations, Kilner expressly discloses "forming a first commutative checksum by a commutative operation on said first checksum, wherein flow control for the data segments is negated by the commutative operation."

In reply to Appellant's argument that the prior art (Kilner combined with the teachings of Frezza) does not render obvious cryptographically protecting the first

commutative checksum (Appeal Brief, pg. 13), cryptographic protection of data values are well recognized techniques in the art to hide the actual value of information from others and/or to prevent the value from being altered using secure operations. For example, the Frezza prior art describes using an encryption technique to secure a checksum value, wherein the checksum is used for verification purposes. See col. 2:45-3:14. Frezza as applied to the teachings of Kilner, suggest that to ensure the integrity of the cumulative checksums, which are used to verify that the records of the standby database are identical to the active database, the cumulative checksums should be encrypted.

Appellant further argues that there is no reason to cryptographically secure the cumulative checksum value of Kilner because Kilner merely discloses a system for internally resolving updates. Appeal Brief, pg. 14, 1st full paragraph. However, contrary to Appellant's allegation, Kilner never suggests that the system is a completely encapsulated internal system. There is no mention of any provisions to segregate the active database and the standby database from the external network. See col. 2, line 57-col. 3, line 32; fig. 1. Even assuming that the system is a completely isolated internal network, this network configuration would not render cryptographic protection of the checksums useless in the Kilner invention. Appellant's rational that an internal network does not require cryptographic protection is predicated on the assumption of an all or nothing security zone. This is never the case. Even a simplified network with only one machine running a UNIX operating system involves a layered protection scheme, i.e. different accounts, different users.

Hence, the step of cryptographically protecting the first commutative checksum using a cryptographic operation would be obvious to one of ordinary skill in the art because it prevents others from altering the commutative checksum.

For the above reasons, it is believed that the rejections should be sustained.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

Respectfully submitted,

/Jung W Kim/
Examiner AU 2132

/Gilberto Barron Jr/
Supervisory Patent Examiner, Art Unit 2132

Conferees:

/G. B./
Supervisory Patent Examiner, Art Unit 2132

Benjamin Lanier
/Benjamin E Lanier/
Primary Examiner, Art Unit 2132